



INSTITUT TEKNOLOGI TELKOM SURABAYA
FAKULTAS TEKNOLOGI INDUSTRI DAN INFORMASI
PROGRAM STUDI S1 TEKNOLOGI INFORMASI

Kode Dokumen

RENCANA PEMBELAJARAN SEMESTER

Mata Kuliah (MK)	Kode MK	Rumpun MK	Bobot (SKS)	Semester	Tanggal Penyusunan
Keamanan Informasi	ITA3223	Manajemen Teknologi Informasi	T=3 P=0	4	26 Maret 2018
OTORISASI/PENGESAHAN	Pengembang RPS	Koordinator RMK	Ketua PRODI		
	Khodijah Amiroh, S.ST.,M.T.	Philip Tobianto Daely, S.T.,M.Eng	Farah Zakiyah R., S.ST.,M.T.		
Capaian Pembelajaran (CP)	CPL-PRODI				
	P12	Menjelaskan konsep dan teori dasar security dari suatu sistem informasi;			
	KK13	Mengidentifikasi ancaman-ancaman jaringan dan penanganannya;			
	KK20	Mengidentifikasi kelemahan dan ancaman dari sebuah arsitektur teknologi informasi;			
	KK21	Menerapkan metode kriptografi sebagai salah satu upaya pengamanan data dan informasi;			
	CP-MK	Mahasiswa mampu :			
	1	Memahami konsep mengenai dasar kriptografi			
	2	Memahami konsep keamanan pada jaringan komputer			
Deskripsi Singkat MK	Membahas mengenai sistem keamanan pada komputer. Tujuan utama dalam mata kuliah ini adalah mengenalkan dasar sistem keamanan, dasar kriptografi, keamanan dalam sebuah program, merancang sistem operasi.				
Materi Pembelajaran/ Pokok Bahasan	<ol style="list-style-type: none"> 1. Pengertian dan fungsi keamanan informasi 2. Konsep VTRC pada keamanan sistem informasi 3. Kriptografi 4. Kendali akses 5. Konsep, fungsi dan aspek keamanan jaringan 6. Keamanan host 7. Keamanan data 8. Keamanan berbasis web 9. Keamanan cloud 10. Keamanan operasional 11. Konsep forensik 				
Pustaka	Utama				

	[1] KodeGL :GTS Learning,"CompTIA Security+ SY0-041 : Official Study Guide", 2015	
	Pendukung	[2] Information Security Laboratory Manual :GTS Learning,"CompTIA Security+ SY0-041 : Official Study Guide", 2015
Media Pembelajaran	Perangkat Keras PC/Laptop	Perangkat Lunak Snort, Wireshark, Tor
Team Teaching	Khodijah Amiroh, S.ST.,M.T.	
Matakuliah Prasyarat	Algoritma dan Pemrograman, Jaringan Komputer, dan Sistem Operasi Komputer	

Minggu ke-	Sub-CPMK (Kemampuan akhir tiap tahapan belajar)	Indikator Penilaian	Kriteria & Bentuk Penilaian	Bentuk, Metode Pembelajaran, dan Penugasan Mahasiswa [Media & Sumber belajar] [Estimasi Waktu]	Materi Pembelajaran [Pustaka]	Bobot Penilaian (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)
1	Mahasiswa mampu menjelaskan pengertian, fungsi dan tujuan keamanan informasi	Ketepatan dalam menjelaskan pengertian, fungsi, dan tujuan keamanan informasi	Kriteria: Rubrik Deskriptif Bentuk Non Test: Resume tentang penjelasan keamanan informasi beserta contoh dan aplikasinya	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-1 : Menyusun ringkasan dalam bentuk makalah tentang keamanan informasi beserta contoh dan aplikasinya [BT+BM:(1+1)x(3x60'')] 		5
2	Mahasiswa mampu menjelaskan konsep vulnerabilities dan threat pada keamanan informasi Mahasiswa mampu menjelaskan konsep risk dan control pada keamanan informasi	Ketepatan dalam menjelaskan konsep vulnerabilities dan threat pada keamanan informasi Ketepatan dalam menjelaskan konsep risk dan control pada	Kriteria: Rubrik Deskriptif Bentuk Non Test: Resume tentang penjelasan vulnerabilities dan threat pada keamanan informasi	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-2 : Menyusun ringkasan dalam bentuk makalah tentang penjelasan vulnerabilities dan 		5

	Mahasiswa mampu mengimplementasikan dan menghasilkan analisa pada berbagai kasus keamanan informasi pada software lab	keamanan informasi Kemampuan dalam mengimplementasikan dan menganalisa berbagai kasus keamanan informasi		threat pada keamanan informasi [BT+BM:(1+1)x(3x60'')]		
3			Kriteria: Rubrik Deskriptif Bentuk Non Test: Melakukan implementasi dan analisa dengan menggunakan software tersedia	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-3 : Melakukan percobaan dan analisa menggunakan software yang tersedia [BT+BM:(1+1)x(3x60'')]		10
4			Kriteria: Rubrik Deskriptif Bentuk Test: Presentasi dari implementasi dan analisa dari kasus keamanan lab yang telah dibuat	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-4 : Melakukan demo dari percobaan dan analisa yang telah dibuat [BT+BM:(1+1)x(3x60'')]		10
5	Mahasiswa mampu menjelaskan pengertian kriptografi Mahasiswa mampu menjelaskan contoh kasus dan implementasi kriptografi pada software lab	Ketepatan dalam menjelaskan pengertian kriptografi Kemampuan dalam mengimplementasikan software lab beserta strategi lab dalam keamanan informasi	Kriteria: Rubrik Deskriptif Bentuk Non Test: Membuat resume dalam menjelaskan pengertian kriptografi	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-5 : Menyusun ringkasan dalam bentuk makalah tentang pengertian kriptografi [BT+BM:(1+1)x(3x60'')]		15
6		pada berbagai studi kasus Kemampuan dalam penggunaan tools dan environment lab keamanan informasi	Kriteria: Rubrik Deskriptif Bentuk Non Test: Melakukan implementasi pada software lab beserta strategi lab dalam keamanan informasi	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-6 : Melakukan percobaan dengan software yang tersedia [BT+BM:(1+1)x(3x60'')]		5

7			Kriteria: Rubrik Deskriptif Bentuk Non Test: Melakukan percobaan dalam penggunaan tools dan environment lab pada keamanan informasi	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-7 : Melakukan percobaan dengan software yang tersedia [BT+BM:(1+1)x(3x60'')] 		10
8	Evaluasi Tengah Semester: Melakukan validasi hasil penilaian, evaluasi dan perbaikan proses pembelajaran berikutnya					
9	Mahasiswa mampu menjelaskan konsep keamanan jaringan Mahasiswa mampu menjelaskan strategi dan implementasi sistem keamanan jaringan Mahasiswa mampu mengimplementasikan dan menghasilkan analisa pada berbagai kasus keamanan informasi pada software lab	Mahasiswa mampu menjelaskan konsep, fungsi, dan aspek keamanan jaringan dengan melakukan desain keamanan jaringan, aplikasi dan perangkat keamanan jaringan, keamanan nirkabel	Kriteria: Rubrik Deskriptif Bentuk Non Test: Membuat resume dalam menjelaskan konsep keamanan jaringan dan strategi dalam implementasi keamanan jaringan	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-8 : Menyusun ringkasan dalam bentuk makalah tentang konsep keamanan jaringan dan strategi dalam implementasi keamanan jaringan [BT+BM:(1+1)x(3x60'')] 		10
10	menghasilkan analisa pada berbagai kasus keamanan informasi pada software lab		Kriteria: Rubrik Deskriptif Bentuk Non Test: Melakukan implementasi dan analisa pada berbagai kasus keamanan informasi pada software lab	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-9 : Melakukan percobaan dengan software tersedia [BT+BM:(1+1)x(3x60'')] 		5
11	Mahasiswa mampu menjelaskan konsep keamanan host Mahasiswa mampu menjelaskan konsep keamanan data Mahasiswa mampu	Mahasiswa mampu menjelaskan keamanan host seperti manajemen hardening, dan konfigurasi host implementasi group policy, manajemen	Kriteria: Rubrik Deskriptif Bentuk Non Test: Membuat resume tentang konsep keamanan host dan konsep keamanan data	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-10 : Menyusun ringkasan dalam bentuk makalah tentang konsep keamanan host dan 		5

	mengimplementasikan dan menganalisa pada berbagai kasus keamanan informasi pada software lab	patches dan update, mengelola network access control Mahasiswa mampu mengimplementasikan keamanan data seperti policy keamanan data, penggunaan enkripsi, pencegahan data loss, backup dan siklus hidup data		konsep kewanaman data [BT+BM:(1+1)x(3x60'')]		
12			Kriteria: Rubrik Deskriptif Bentuk Non Test: Membuat sistem keamanan, mengimplementasikan, serta menganalisa berbagai kasus keamanan informasi pada software lab	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-11 : Melakukan percobaan dengan software tersedia [BT+BM:(1+1)x(3x60'')] 		5
13	<p>Mahasiswa mampu menjelaskan konsep dan implementasi keamanan aplikasi berbasis web</p> <p>Mahasiswa mampu menjelaskan konsep dan implementasi keamanan cloud</p> <p>Mahasiswa mampu menjelaskan konsep dan implementasi keamanan mobile</p> <p>Mahasiswa mampu mengimplementasikan dan menghasilkan analisa pada berbagai kasus keamanan informasi pada software lab</p>	<p>Ketepatan dalam melakukan keamanan berbasis web seperti keamanan aplikasi web, keamanan web services, teknologi SSL, konsep keamanan pada mobile, keamanan web server</p> <p>Ketepatan dalam melakukan keamanan cloud seperti keamanan virtualisasi, isu keamanan cloud</p>	Kriteria: Rubrik Deskriptif Bentuk Non Test: Membuat resume dalam konsep keamanan aplikasi berbasis web, keamanan cloud, keamanan mobile, dan mengimplementasikan serta menganalisa pada berbagai kasus keamanan informasi pada software lab	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-12 : Menyusun ringkasan dalam bentuk makalah tentang konsep keamanan aplikasi berbasis web, keamanan cloud, keamanan mobile, dan mengimplementasikan serta menganalisa pada berbagai kasus keamanan informasi pada software lab [BT+BM:(1+1)x(3x60'')] 		5
14	<p>Mahasiswa mampu menjelaskan pengertian, fungsi, dan contoh kebijakan, program, operasional keamanan informasi</p> <p>Mahasiswa mampu menjelaskan manajemen resiko keamanan dan</p>	<p>Ketepatan dalam keamanan operasional seperti aspek akses dan keamanan fosok, manajemen resiko keamanan, kontinuitas bisnis, business impact</p>	Kriteria: Rubrik Deskriptif Bentuk Non Test: Melakukan resume beserta menjelaskan pengertian, fungsi dan contoh	<ul style="list-style-type: none"> • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-13 : Menyusun ringkasan dalam bentuk makalah tentang menjelaskan pengertian, 		5

	kontinuitas bisnis Mahasiswa mampu menjelaskan pengelolaan respon insiden dan aspek forensik	analysis, disaster recovery planning Ketepatan dalam pengelolaan dan tanggung jawab respon insiden konsep Ketepatan dalam menjelaskan konsep forensic seperti karakteristik investigasi forensik	kebijakan, program, operasional keamanan informasi Kriteria: Rubrik Deskriptif Bentuk Non Test: Melakukan resume tentang manajemen resiko keamanan dan kontinuitas bisnis serta pengelolaan respon insiden dan aspek forensik	fungsi dan contoh kebijakan, program, operasional keamanan informasi [BT+BM:(1+1)x(3x60'')] • Kuliah • Diskusi [TM:1x(3x50'')] • Tugas-14 : Menyusun ringkasan dalam bentuk makalah tentang manajemen resiko keamanan dan kontinuitas bisnis serta pengelolaan respon insiden dan aspek forensik [BT+BM:(1+1)x(3x60'')]		
15						5
16	Evaluasi Akhir Semester: Melakukan validasi penilaian akhir dan menentukan kelulusan mahasiswa					
Catatan: (1). TM: Tatap Muka; TS: Penugasan Terstruktur; BM: Belajar Mandiri. (2). 1 sks = (50' TM + 50' PT + 60' BM)/Minggu (3). CPL-Prodi: Capaian Pembelajaran Lulusan Program Studi; CP-MK: Capaian Pembelajaran Mata-Kuliah (4). Simbol-simbol elemen KKNI pada CPL-Prodi: S = Sikap; KU = Ketrampilan Umum; KK = Ketrampilan Khusus; P = Pengetahuan						



INSTITUT TEKNOLOGI TELKOM SURABAYA

FAKULTAS

PRODI STUDI

RENCANA TUGAS MAHASISWA

Mata Kuliah (MK)	Kode MK	Rumpun MK/Kelompok Keahlian (KK)	Bobot (SKS)	Semester	Tahun Akademik
	
Dosen Pengampu					
TUGAS KE-	JUDUL TUGAS				
...	...				
SUB-CAPAIAN PEMBELAJARAN MATA-KULIAH					
TUJUAN PENUGASAN					
DESKRIPSI TUGAS			METODE Pengerjaan Tugas		
1. Objek Garapan: 2. Batasan: 3. Relevansi: 4. Manfaat: 5. ...			1. 2. 3.		
BENTUK DAN FORMAT LUARAN TUGAS			INDIKATOR, KRITERIA DAN BOBOT PENILAIAN		
1. ... 2. ...					
JADWAL PELAKSANAAN TUGAS			CATATAN /LAIN-LAIN		
DAFTAR RUJUKAN					
1.					